UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/821,482	04/09/2004	Barry Steven Herman	L111US	1214

30368 7590 12/05/2008
Theodore A. Chen
EMC Corporation
6801 Koll Center Parkway
Pleasanton, CA 94566

EXAMINER	
LOUIE, OSCAR A	
ART UNIT	PAPER NUMBER
2436	
MAIL DATE	DELIVERY MODE
12/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.**	**Applicant(s)**	
	10/821,482	HERMAN, BARRY STEVEN	
	Examiner	**Art Unit**	
	OSCAR A. LOUIE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 September 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,5-10 and 12-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,5-10 and 12-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 09/04/2008. Claims 1, 3, 5-10, & 12-20 are pending and have been considered as follows.

Examiner Note

In view of the applicant's amendments, the examiner hereby withdraws his previous Specification Objection with respect to Claim 16 and withdraws his previous Claim Objections with respect to Claims 1, 9, & 16.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 9 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

- Claim 9 recites a system that performs function steps but without any mention of hardware or some structure that performs these function steps.
    - The examiner notes that unless clearly defined in the applicant's Specification/original disclosure, "computer" does not clearly define a computer device comprising a processor and memory with instructions stored on the

memory that once executed by the processor perform method steps; that is, a "computer" unless clearly defined could merely be a virtual machine, thereby being only software;

See, e.g., Rubber-Tip Pencil Co. v. Howard, 87 U.S. (20 Wall.) 498, 507 (1874) ("idea of itself is not patentable, but a new device by which it may be made practically useful is"); Mackay Radio & Telegraph Co. v. Radio Corp. of America, 306 U.S. 86, 94, 40 USPQ 199, 202 (1939) ("While a scientific truth, or the mathematical expression of it, is not patentable invention, a novel and useful structure created with the aid of knowledge of scientific truth may be."); Warmerdam, 33 F.3d at 1360, 31 USPQ2d at 1759 ("steps of locating' a medial axis, and creating' a bubble hierarchy . . . describe nothing more than the manipulation of basic mathematical constructs, the paradigmatic abstract idea'")

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3, 5-10, & 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raith (US-5241598-A) in view of Hatta (US-5115508-A) and in further view of Banes et al. (US-20030182584-A1).

Claim 1:

Raith discloses a method of resetting a key for accessing a computer program comprising,

- "setting a flag to indicate that the key is to be reset" (i.e. "including in a message sent from the network to the mobile station an order or a signal (flag) to reset the B-key") [column 30 lines 52-53];

- "starting a process associated with the program" (i.e. "Execution of the authentication algorithm in the home network") [column 17 lines 37-38];
- "determining, after the process has been started, whether the flag is set" (i.e. "The network may reset the B-key value in the network to the selected value immediately before or at the time of activating the B-key step flag, i.e., setting the bit-value equal to 1 for example, in an order message sent to the mobile station or immediately after receiving from the mobile station an acknowledgement of the order message") [column 30 lines 65-68 & column 31 lines 1-3];
- "resetting the key to a default value based on the flag" (i.e. "According to the present invention, resynchronization of the B-key used by the network and the mobile station may be accomplished by resetting the B-key input to AUTH in each of the network and the mobile station to a selected value") [column 30 lines 38-42];

but, Raith does not explicitly disclose,

- "wherein the flag comprises an environment variable stored at a computer on which the computer program is installed," although Hatta does suggest storing a flag and Banes et al. do suggest a reset flag, as recited below;
- "determining whether the flag is set comprises reading the environment variable," although Hatta does suggest judging a flag to make a decision, as recited below;

- "a prescribed level of privilege with respect to the computer is required to set the flag and start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value," although Banes et al. do suggest password resetting without the aid of a third party, as recited below;

however, Hatta does disclose,

- "store writing prohibition flag WRP" [column 3 line 4];
- "the condition of the password setting flag PASF1 is judged" [column 3 lines 35-36];

whereas, Banes et al. do disclose,

- "The B-key reset flag may consist of any number of bits and, in the simplest case, may be no more than a single bit (1 or 0) assigned to a specific field in the message transmitted from the network to the mobile station" [column 30 lines 61-64];
- "implementations creating a password reset disk and using the password reset disk to reset a user password in a computer system are shown. Utilizing the described systems and methods a user can create a password reset disk that--in the event that the user forgets her password --can be used to securely create a new password for the user without the user having to contact a third party" [page 1 para 9 lines 1-7];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the flag comprises an environment variable stored at a computer on which the computer program is installed" and "determining whether the flag is set comprises reading the environment variable" and "a prescribed level of privilege with respect to the computer is required to set the flag and start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value," in the invention as disclosed by Raith for the purposes of storing a flag value and permitting a user to reset their password without intervention of a third party.

Claim 3:

Raith, Hatta, and Banes et al. disclose a method of resetting a key for accessing a computer program, as in Claim 1 above, further comprising,

- "logging in with, sufficient privileges to start the process" (i.e. "To guard against this risk, the performance of a B-key reset may be linked to the performance of bilateral authentication, i.e., to the validation of the network") [column 32 lines 4-7].

Claim 5:

Raith, Hatta, and Banes et al. disclose a method of resetting a key for accessing a computer program, as in Claim 1 above, further comprising,

- "resetting the key to a default value includes instructing a database system to reset the key" (i.e. "According to the present invention, resynchronization of the B-key used by the network and the mobile station may be accomplished by resetting the B-key input to AUTH in each of the network and the mobile station to a selected value" [column 30 lines 38-42].

Claim 6:

Raith, Hatta, and Banes et al. disclose a method of resetting a key for accessing a computer program, as in Claim 1 above, further comprising,

- "unsetting the flag" (i.e. "The B-key reset flag may consist of any number of bits and, in the simplest case, may be no more than a single bit (1 or 0) assigned to a specific field in the message transmitted from the network to the mobile station") [column 30 lines 61-64].

Claim 7:

Raith, Hatta, and Banes et al. disclose a method of resetting a key for accessing a computer program, as in Claim 6 above, further comprising,

- "starting the process again" (i.e. "When the mobile subscriber crosses over into another area, the exchange associated with that area, upon receiving an identity signal from the telephone unit, will record an indication of the mobile subscriber's presence there and then transmit the identity signal to all of the other exchanges together with its own identity signal, for the purpose of updating the mobile subscriber's position") [column 2 lines 59-66].

Claim 8:

Raith, Hatta, and Banes et al. disclose a method of resetting a key for accessing a computer program, as in Claim 6 above, further comprising,

- "changing the key from the default value to a secure value" (i.e. "Where encryption is desired, a new S-key must be calculated since the previous S-key was calculated using the previous B-key which was out of synchronization") [column 31 lines 10-13].

Claims 9:

Raith discloses a system configured to reset a key for accessing a computer program, comprising a computer, comprising a computer comprising,

- "determine whether a flag is set, after a process associated with the computer program is started" (i.e. "The network may reset the B-key value in the network to the selected value immediately before or at the time of activating the B-key step flag, i.e., setting the bit-value equal to 1 for example, in an order message sent to the mobile station or immediately after receiving from the mobile station an acknowledgement of the order message") [column 30 lines 65-68 & column 31 lines 1-3];
- "reset the key to a default value, based on the flag" (i.e. "According to the present invention, resynchronization of the B-key used by the network and the mobile station may be accomplished by resetting the B-key input to AUTH in each of the network and the mobile station to a selected value") [column 30 lines 38-42];

but, Raith does not disclose,

- "wherein the flag comprises an environment variable stored on the computer," although Hatta does suggest storing a flag and Banes et al. do suggest a reset flag, as recited below;
- "the computer is configured to determine whether the flag is set by reading the environment variable," although Hatta does suggest judging a flag to make a decision, as recited below;

- "a prescribed level of privilege with respect to the computer is required to set the flag and start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value," although Banes et al. do suggest password resetting without the aid of a third party, as recited below;

however, Hatta does disclose,

- "store writing prohibition flag WRP" [column 3 line 4];
- "the condition of the password setting flag PASF1 is judged" [column 3 lines 35-36];

whereas, Banes et al. do disclose,

- "The B-key reset flag may consist of any number of bits and, in the simplest case, may be no more than a single bit (1 or 0) assigned to a specific field in the message transmitted from the network to the mobile station" [column 30 lines 61-64];
- "implementations creating a password reset disk and using the password reset disk to reset a user password in a computer system are shown. Utilizing the described systems and methods a user can create a password reset disk that--in the event that the user forgets her password --can be used to securely create a new password for the user without the user having to contact a third party" [page 1 para 9 lines 1-7];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the flag comprises an environment variable stored on the computer" and "the computer is configured to determine whether the flag is set by reading the environment variable" and "a prescribed level of privilege with respect to the computer is required to set the flag and start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value," in the invention as disclosed by Raith for the purposes of storing a flag value and permitting a user to reset their password without intervention of a third party.

Claim 10:

Raith, Hatta, and Banes et al. disclose a system configured to reset a key for accessing a computer program, comprising a computer, as in Claim 9 above, further comprising,

- "configured to require administrator privileges to start the process" (i.e. "To guard against this risk, the performance of a B-key reset may be linked to the performance of bilateral authentication, i.e., to the validation of the network") [column 32 lines 4-7].

Claim 12:

Raith, Hatta, and Banes et al. disclose a system configured to reset a key for accessing a computer program, comprising a computer, as in Claim 9 above, further comprising,

- "a database system configured to store the key" (i.e. "the HLR has no voice transmission, reception or switching facilities, but is essentially a database from and to which information can be read and written") [column 15 lines 7-9];
- "the system is configured to reset the key by instructing the database system to reset the key" (i.e. "the network can retrieve information pertaining to that particular mobile station, e.g., security keys, from the location or database") [column 15 line 68 & column 16 lines 1-2].

Claim 13:

Raith, Hatta, and Banes et al. a system configured to reset a key for accessing a computer program, comprising a computer, comprising a computer, as in Claim 9 above, further comprising,

- "the key is associated with an administrator account for accessing the computer program" (i.e. "To guard against this risk, the performance of a B-key reset may be linked to the performance of bilateral authentication, i.e., to the validation of the network") [column 32 lines 4-7].

Claim 14:

Raith, Hatta, and Banes et al. disclose a system configured to reset a key for accessing a computer program, comprising a computer, as in Claim 9 above, further comprising,

- "the computer program executes on the computer" (i.e. "an authentication algorithm executed in each of the mobile station and the network") [column 7 lines 62-64].

Claim 15:

Raith, Hatta, and Banes et al. disclose a system configured to reset a key for accessing a computer program, comprising a computer, as in Claim 9 above, further comprising,

- "the computer program executes on a second computer" (i.e. "an authentication algorithm executed in each of the mobile station and the network") [column 7 lines 62-64].

Claim 16:

Raith discloses a computer program product configured to reset a key for accessing a computer program, comprising a computer readable storage medium having machine readable code embodied therein comprising,

- "determining whether a flag is set, after a process associated with the computer program is started" (i.e. "The network may reset the B-key value in the network to the selected value immediately before or at the time of activating the B-key step flag, i.e., setting the bit-value equal to 1 for example, in an order message sent to the mobile station or immediately after receiving from the mobile station an acknowledgement of the order message") [column 30 lines 65-68 & column 31 lines 1-3];
- "resetting the key to a default value, based on the flag" (i.e. "According to the present invention, resynchronization of the B-key used by the network and the mobile station may be accomplished by resetting the B-key input to AUTH in each of the network and the mobile station to a selected value") [column 30 lines 38-42];

but, Raith does not disclose,

- "wherein the flag comprises an environment variable stored at a computer on which the computer program is installed," although Hatta does suggest storing a flag and Banes et al. do suggest a reset flag, as recited below;
- "determining whether the flag; is set comprises reading the environment variable," although Hatta does suggest judging a flag to make a decision, as recited below;
- "a prescribed level of privilege with respect to the computer is required to set the flag and start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value," although Banes et al. do suggest password resetting without the aid of a third party, as recited below;

however, Hatta does disclose,

- "store writing prohibition flag WRP" [column 3 line 4];
- "the condition of the password setting flag PASF1 is judged" [column 3 lines 35-36];

whereas, Banes et al. do disclose,

- "The B-key reset flag may consist of any number of bits and, in the simplest case, may be no more than a single bit (1 or 0) assigned to a specific field in the message transmitted from the network to the mobile station" [column 30 lines 61-64];
- "implementations creating a password reset disk and using the password reset disk to reset a user password in a computer system are shown. Utilizing the described systems and methods a user can create a password reset disk that--in the event that the user forgets her password --can be used to securely create a new password for the user without the user having to contact a third party" [page 1 para 9 lines 1-7];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the flag comprises an environment variable stored at a computer on which the computer program is installed" and "determining whether the flag; is set comprises reading the environment variable" and "a prescribed level of privilege with respect to the computer is required to set the flag and start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value," in the invention as disclosed by Raith for the purposes of storing a flag value and permitting a user to reset their password without intervention of a third party.

Claim 17:

Raith, Hatta, and Banes et al. disclose a computer program product configured to reset a key for accessing a computer program, comprising a computer readable storage medium having machine readable code embodied therein, as in Claim 16 above, further comprising,

- "a database system configured to store the key" (i.e. "the HLR has no voice transmission, reception or switching facilities, but is essentially a database from and to which information can be read and written") [column 15 lines 7-9];
- "resetting the key includes instructing the database system to reset the key" (i.e. "the network can retrieve information pertaining to that particular mobile station, e.g., security keys, from the location or database") [column 15 line 68 & column 16 lines 1-2].

Claim 18:

Raith, Hatta, and Banes et al. disclose a computer program product configured to reset a key for accessing a computer program, comprising a computer readable storage medium having machine readable code embodied therein, as in Claim 16 above, further comprising,

- "the key is associated with an administrator account for accessing the computer program" (i.e. "To guard against this risk, the performance of a B-key reset may be linked to the performance of bilateral authentication, i.e., to the validation of the network") [column 32 lines 4-7].

Claim 19:

Raith, Hatta, and Banes et al. disclose a computer program product configured to reset a key for accessing a computer program, comprising a computer readable storage medium having machine readable code embodied therein, as in Claim 16 above, further comprising,

- "code for requiring sufficient privileges to start the process" (i.e. "To guard against this risk, the performance of a B-key reset may be linked to the performance of bilateral authentication, i.e., to the validation of the network") [column 32 lines 4-7].

Claim 20:

Raith, Hatta, and Banes et al. disclose a computer program product configured to reset a key for accessing a computer program, comprising a computer readable storage medium having machine readable code embodied therein, as in Claim 16 above, further comprising,

- "code for changing the key from the default value to a secure value" (i.e. "Where encryption is desired, a new S-key must be calculated since the previous S-key was calculated using the previous B-key which was out of synchronization") [column 31 lines 10-13].

Response to Arguments

4. Applicant's arguments filed 09/04/2008 have been fully considered but they are not persuasive.

- The applicant's arguments, "the signal taught by Raith is not a "flag" within the meaning of the claim because it is not an environment variable that is subsequently read to determine whether it has been set to a value indicating that the key should be reset to the default value" and "Hatta and Banes likewise do not describe a flag that is an "environment variable" stored on a computer with which the recited computer program is associated" and "The flags described by Hatta are not used to reset a password to a default value, as recited in claims 1, 9, and 16, but rather to ensure that only holders of the password(s) are allowed to perform certain operations," has been carefully considered but is non-persuasive.

- The examiner notes that the prior art may not use the exact same claim language as "environment variable," but the "flag" still functions in the same way as the applicant's "variable"; unless there is further clarification as to what the "environmental variable" comprises to distinguish itself from the prior art, the broadest most reasonable interpretation would include any value/variable, thus a "flag" which acts similarly would be seen by one of ordinary skill in the art as obvious; it is also noted, that the purpose of the "environment variable" can be construed as merely intended use, whereas the method in which the variable is used resulting in a tangible outcome/transformation may be a novelty;

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
11/25/2008

/Carl Colin/
Primary Examiner, Art Unit 2436
12/1/2008